A RICOH Company

29 January 2026

TenableOne MTI Vulnerability Management Service

Ref no: G-Cloud 15

PREPARED BY

MTI Technology

COPYRIGHT

TABLE OF CONTENTS

1.0 INTRODUCTION

Our Managed Vulnerability Assessment Service (MVAS) delivers continuous, centralised risk assessment, quantification, and measurement across your digital estate. Leveraging the Tenable One platform, our service provides end-to-end vulnerability management, integrating asset discovery, prioritisation, remediation tracking, threat intelligence, and compliance reporting into a single managed solution.

Key Features

- **Centralised Vulnerability Visibility**: Unified dashboards and tailored reports present comprehensive asset and vulnerability data, enabling efficient oversight and informed decision-making.
- **Regular/Continuous Asset Discovery**: Ongoing identification and onboarding of new assets ensure persistent visibility throughout organisational changes, cloud adoption, and business growth.
- **Risk-Based Prioritisation**: Vulnerabilities are triaged using real-world threat intelligence and Vulnerability Priority Rating (VPR), focusing remediation on issues most likely to be exploited.
- **Stakeholder Collaboration**: Asset-based dashboards and reports foster effective communication between IT, security, and business units through sharing vulnerability information relevant to asset owners and allocated resolver groups.
- **Automated Threat Intelligence**: Integration of live threat data underpins proactive vulnerability prioritisation and timely alerting to emerging risks.
- **Regulatory Compliance Support**: VA reports can be used to support compliance efforts for GDPR, NIS 2, PCI-DSS, ISO 27001, Cyber Essentials, CAF, and other standards.
- **Platform Integration**: Managed scanning for on-premises, hybrid, and cloud environments. Capabilities extend to web application and attack surface management, with pre-built templates for best practice configuration and compliance.
- **Expert Management**: The Full Managed Service includes scan configuration, execution, policy tuning, and review of findings, ensuring ongoing alignment with business and regulatory requirements.

Service Outcomes and Benefits

- **Risk Reduction**: Accelerates identification and remediation [by the Customer and resolver teams] of exploitable vulnerabilities, reducing exposure to compromise.
- **Operational Efficiency**: Streamlines vulnerability management workflows, minimising time to remediate critical issues.
- **Security Posture Maturity**: Drives continual improvement through actionable remediation insights, measurable KPIs, and industry benchmarking.
- **Compliance Assurance**: Simplifies evidence gathering for audits, regulatory and statutory obligations.
- **Business Alignment**: Delivers targeted reporting to business and technical stakeholders, underpinning risk-based decision-making and supporting effective and timely resource allocation.

2.0 MANAGED VULNERABILITY ASSESSMENT SERVICE

Through our Managed Vulnerability Assessment (VA) platform and services, the Customer's environments can be regularly/continuously analysed and assessed hand in hand with dynamic or ephemeral changes within cloud instances, containers, virtual machines, web applications and mobile devices, helping to ensure comprehensive visibility of vulnerabilities enabling the Customer to organise timely response and remediation through findings prioritised based on business criticality of assets, and real-world vulnerability exploit potential, not just generic Common Vulnerability Scoring System (CVSS) vulnerability ratings.

Successful mitigation and risk management is achieved by focusing on those vulnerabilities that pose the greatest risk to your organisation and answering the "what should we fix first?" challenge

Our vulnerability assessment services include the following modules:

- **External Vulnerability Assessments (eVA)** – Assesses all public Internet-facing assets, IP addresses and domains vulnerabilities helping to reduce the risk of your business-critical assets being compromised. Detects vulnerabilities including open ports, application-level weaknesses and weak credentials for protocols including SMTP, POP3, HTML, and VPNs through unauthenticated assessment.

- **Attack Surface Management (ASM)** – ASM addresses the gap between known and unknown external IT assets that exist within customer domains, providing a unified 'single source of truth' view and addressing the "you can't protect what you can't see" challenge. Available as an add-on module, licenced by the number of observable objects you wish to monitor such as domain names, subdomains, or IP addresses for internet-connect or internal network devices, with scanning conducted based on the Customer's chosen cadence, daily or fortnightly. Deployment and management of ASM by MTI enables the Customer to:

    - Access comprehensive inventories of internet-facing assets related to the Customer with extensive metadata (circa 180–200 fields), including domains, subdomains, IP addresses, and associated business context.
    - Receive notifications and alerts for changes in the attack surface, such as new assets, open ports, or required patches.
    - Leverage advanced filtering, tagging, and categorization to organize and prioritize assets based on risk and business context. Export reports and conduct granular queries for deeper investigation and integration with other security workflows. For example, searching for newly created SSL/TLS certificates that are subdomains of your corporate domain, that are either newly created or due to expire.

- **Internal Vulnerability Assessments (iVA)** – Assesses internal assets, helping to ensure that your business-critical internal systems cannot be compromised if an attacker was to gain a foothold within your corporate environment.
  MTI's Cyber Security team create, setup, run, monitor, and manage your VA scans and/or Attack Surface Management (ASM), providing reports based on an agreed cadence, and fine-tuning scans and scan policies based on ongoing customer requirements.

- **Network Discovery Scans -** The Tenable Vulnerability Management platform provides the ability to scan known external and internal IP address ranges to detect the presence of IP hosts/ Assets. Any identified assets not receiving vulnerability assessment scanning can be imported into the applicable scan profile/policy and included in regular scanning (consuming an asset license).

- **Tenable Web Application Scanning (WAS)** – MTI set up, configure and manage the WAS module to provide automated, dynamic security testing for web applications, delivering thorough vulnerability detection with minimal false positives. It covers OWASP vulnerabilities and modern dynamic web frameworks (such as HTML5, JavaScript, and AJAX frameworks) and ensures safe, non-disruptive scanning, and integrates seamlessly with the Tenable One platform.

- **Tenable Cloud Security – (TCS)** MTI set up, configure and manage the comprehensive Cloud-Native Application Protection Platform (CNAPP) under the *Tenable Cloud Security - Standard* license*,* helping to secure the Customer's Azure and AWS cloud environments by providing continuous assessment of cloud configurations, protection for workloads, management of identities and access, security for Infrastructure as Code, Kubernetes security posture management, and threat detection and response.

- **Leveraging and Management of Tenable One Bundled Components –** working in close collaboration with the Customer, MTI will configure, manage and highlight the outputs from the additional *bundled-in* components within Tenable One that combine to increase the awareness of threats and vulnerabilities and better helps to understand and track vulnerability and remediation performance, and trends including:
    - Lumin
    - Lumin Exposure view
    - Asset Inventory & Tagging
    - Threat Intelligence
    - Attack Path Analysis
    - Vulnerability Priority Rating (VPR) [Risk based vulnerability scoring]

  Picking just two use cases from the above:

    - Lumin Exposure View enables the Customer to set and monitor custom remediation targets for vulnerabilities in line with NCSC guidelines, such as remediating critical issues within 14 days. It provides clear visualisation of SLA performance, allows segmentation by business unit or asset owner, and offers benchmarking and detailed tracking to ensure vulnerabilities are addressed within required timeframes, supporting compliance and accountability.
    - Tenable's Vulnerability Priority Rating (VPR) will benefit the Customer by enabling you to focus remediation efforts on the vulnerabilities that pose the greatest real-world risk. Unlike traditional scoring systems that rely solely on technical severity, VPR combines technical impact with dynamic threat intelligence—such as exploit availability, active attacks, and emerging threats—to predict the likelihood of exploitation in the near term.

3.0 INITIAL ONBOARDING (PROFESSIONAL SERVICES)

The service onboarding process is first conducted as a professional services engagement scoped to the particular needs of each customer, on a case by case basis, scoped to include for the design, implementation and documentation of the required use cases and the TenableOne component products the customer wishes to consume from their TenableOne asset license. The cost for this professional services engagement is scoped separately from the cost of the managed service, and includes the following steps:

- **Confirm Scope and Prerequisites -** Define in-scope assets and environments, review module licensing entitlements, validate stakeholder contacts, and ensure required network and credential access is available for all targets.
- **Provision Tenable One Platform -** Set up the Tenable One tenancy, configure user access, apply security settings (such as Single-Sign-On [SSO] and data residency), and establish foundational platform controls.
- **Onboard and Discover Assets -** Import and group all relevant assets (internal, external, cloud, web etc.), work with the Customer to deploy scanning agents, scanning engines, configure connectors/integrations, and run discovery scans to ensure comprehensive coverage.
- **Configure and Schedule Scans -** Create and tune scan policies, assign scan targets and schedules, apply relevant templates, exclusion lists, and authentication settings, and enable real-time alerting.
- **Execute Baseline Scans and Validate Outputs** - Run initial scans, review results with stakeholders for completeness and accuracy, and tune policies as required.

Once the initial onboarding activities are completed, the customer will be transitioned to the *Vulnerability Management Service*

4.0 ONGOING SCAN MANAGEMENT

After the initial onboarding, MTI takes on responsibility for managing the Customer's vulnerability scans, including:

- Setup of vulnerability scans based on a the Customer's requirement for continuous, or frequency-based vulnerability scans
- Setup of proactive alerting and customer notifications
- Scan monitoring, ensuring that scans are successfully undertaken and completed, liaising with relevant teams at the Customer to resolve any issues associated with scanning, and production of reports.
- Ensuring that vulnerability reports are sent to and received by authorised/designated recipients
- Ensuring that vulnerability dashboards are configured and available to authorised/designated recipients
- On a weekly/monthly/quarterly basis meet with the customer to review the scans, their scan schedules, any risk acceptance or removed assets, and document and implement any required changes.
- Where requests to exclude assets from scans or accept risks are received, these requests will only be actioned when made by an authorised person and will be documented within our ITSM platform and monthly report along with the date, the reason(s), the authoriser, and a next review date.
- On a weekly/monthly basis MTI meets with the Customer's nominated staff to review the vulnerabilities highlighted, the vulnerability trends, escalated work, and other salient matters.
- In the event of the Customer identifying a risk to them resulting from a critical vulnerability 'in the wild,' the Customer can request tactical scans and ad-hoc changes by contacting the MTI Service Desk.

- the Customer can request tactical scans to support BAU vulnerability management processes, for example, running a VA scan on a host before being moved into production use, by contacting the MTI Service Desk.

5.0 SCANNING SCHEDULE

MTI's standard is to set up the scanning cadence as per the below schedule. MTI will work with the Customer to establish the correct level of scans and frequencies.

Scan Type	Frequency
Tenable Platform	Always On
Agents (User end points)	Monday to Friday (During Business Hours)
Agents (Servers)	Daily (Outside business hours)
Internal Network	Weekly (Outside business hours)
External Network	Daily (Outside business hours)
Passive	Always on
Agentless (AWS / Azure)	Daily (Outside business hours)

6.0 REQUIREMENTS OF THE SERVICE

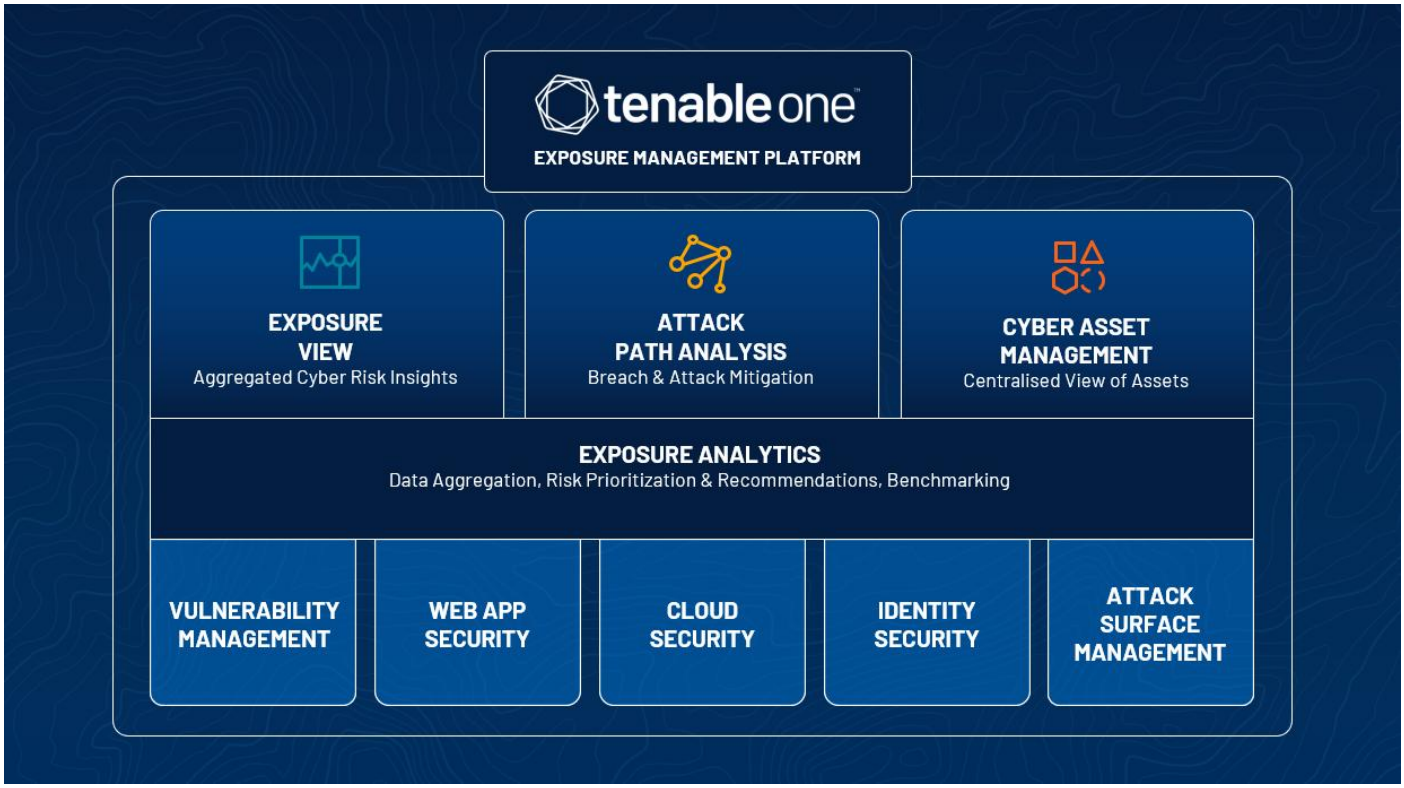
Customers subscribing to this service require or are governed by the following:

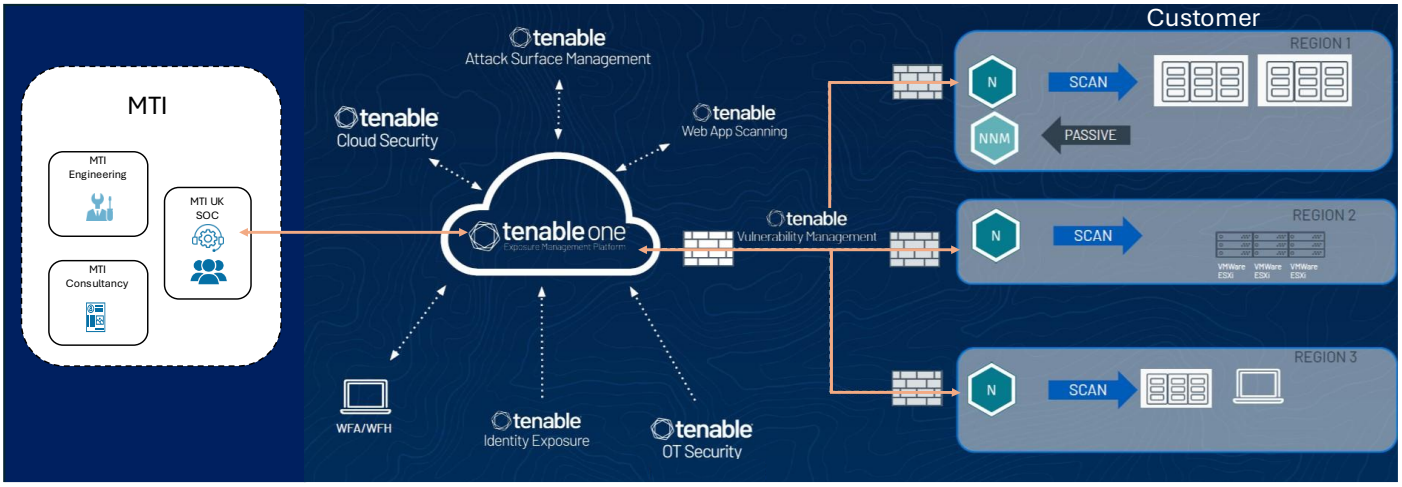
- Obtaining and providing the permission to scan hosts within any multi-tenant environments
- Tagging of assets based on business criticality to help with effective prioritisation
- the Customer is responsible for deployment of any required agents to hosts using their existing software deployment tooling. MTI will provide instructions, prerequisites, and guidance for deployment of relevant Tenable agents.

7.0 TENABLE ONE PLATFORM OVERVIEW

The Vulnerability Management Service is powered by Tenable and provides a class leading vulnerability scanning and management solution, providing the tools and functionality to deliver vulnerability assessments, and the insights necessary to advance your security posture and safeguard your business.

The Tenable platform is evergreen and continually updated with new vulnerability definitions and checks, zero-day research, and compliance benchmarks. Customers also receive functionality updates as and when they are released.





The Tenable platform provides:

- **Cloud visibility:** visibility and assessment of your external assets within public cloud environments such as AWS, Azure, GCP using Cloud connectors
- **Asset-based vulnerability tracking:** provides the ability to track assets and their vulnerabilities through their life of change. Find vulnerabilities such as misconfigurations, missing patches, encryption weaknesses, and application bugs including for example OWASP Top 10 issues such as SQL injection, cross-site scripting, services listening on unsecured transfer protocols, servers configured with deprecated services (SSL, TLS 1.0, TLS 1.1) and more. Identify any services or new servers that have been set up since the last scan and identify if they present any new threats to your organisation.
- **Best Practice Templates:** the platform includes pre-defined scanning templates and configuration audit checks that follow best practice standards such as CIS, DISA, STIG to help protect the Customer. MTI can customise reporting and analysis with pre-configured dashboards to meet organisational needs.
- **Exclusion lists:** assets can be excluded from scanning where necessary, to reduce noise and keep within asset license.
- **Compliance:** our solution is a PCI Council certified Approved Scanning Vendor (ASV) and can be used to provide ASV scans if the additional PCI ASV license option is purchased.
- **Proactive Alerting:** When a new vulnerability is discovered and Tenable releases updated plugins/checks, we can configure your Tenable instance to proactively scan your systems and alert asset owners/resolvers to newly discovered vulnerabilities automatically.
- **Scan Types:** Scans can be undertaken through either agent-based, passive, active, or connectors. Frictionless assessments work through API integration and the use of native resources such as automation runbooks to collect data. Scans can be run continuously for supported platforms, as well as scheduled, or via ad-hoc scanning.
- **Live Results -** Tenable One's *Live Results* feature enables security teams to immediately assess whether a newly published vulnerability exists within their asset inventory without waiting for the next scheduled scan, using up-to-date vulnerability checks.

The Tenable One platform can scan external/Internet systems, on-premises systems, Cloud, SaaS, IoT, and OT environments and components including but not limited to:

Cloud	On-Premises Infrastructure	Bundled-in Tooling	Additional Modules
Azure VM – Windows	Laptop/Desktop – Windows	Lumin	Tenable Cloud Security
Azure VM – Linux	Laptop/Desktop – Linux	Lumin Exposure view	Web application
Azure IAC/Container	Laptop/Desktop – MacOS	Asset Inventory & Tagging	Attack Surface Management
AWS VM – Windows	VM/Server – Windows	Threat Intelligence	PCI ASV
AWS VM – Linux	VM/Server – Linux	Attack Path Analysis	Active Directory / Identity Exposure
AWS IAC / Container	Switches, Routers, Firewalls	Vulnerability Priority Rating (VPR)	IoT/OT Security

APPENDICES

8.0 APPENDIX – MANAGED VA SERVICE DELIVERABLES MATRIX

The following items are included in the Managed Vulnerability Assessment Service:

Service	Deliverables	Fully Managed
INITIAL (ONCE OFF) DEPLOYMENT & CONFIGURATION	Scope Definition (Assets, Environments, Licenses)	**Out of Scope** of Managed Service – Initial design, install and documentation for greenfield deployments is delivered during an initial Professional Services Engagement
	Prerequisites (Contacts, Host, Network, Cloud and Credential Access)	
	Platform Provisioning and Security Configuration	
	Asset Onboarding and Initial Discovery Scan	
	Scan Policy Configuration and Scheduled Scans	
	Baseline Scanning and Output Validation	
SERVICE LEVEL MANAGEMENT	Tenable Dashboard Access	✓
	Out of the box standard reports	✓
	Defined SLA's	✓
	Reported against SLA Adherence	✓
	Service Delivery Manager with regular customer cadence	**Monthly**
EVENT MANAGEMENT	Monitor the status of the customer Vulnerability environment using the Tenable platform	✓
	Monitor health status of scan servers deployed	✓
	Monitor health status of scan agents deployed	✓
	Monitor the Vulnerability scans for timely completion	✓
	Continuous Monitoring: Ongoing monitoring for new vulnerabilities and emerging threats.	✓
	Cloud and Container Security: Scanning of cloud assets and container environments to identify vulnerabilities and misconfigurations.	✓

Service	Deliverables	Fully Managed
	Detailed Remediation Guidance: Providing clear and actionable remediation steps based on Tenable's findings.	✓
REPORT MANAGEMENT	Volume of Vulnerabilities discovered	✓
	Reporting through Dashboards of (Open, or Resolved & Aged vulnerabilities)	✓
	Service and Commercial Performance	✓
	License capacity review	**Monthly**
	Feature and Functionality enhancements	✓
	Compliance Reporting: Custom reports to demonstrate compliance with standards such as PCI-DSS, HIPAA, GDPR, and others.	✓
	Customizable Reports: Tailored reports to meet specific organizational needs and requirements aligned with assigned asset owners	✓
CAPACITY MANAGEMENT	Host Discovery for asset additions/deletions against contracted asset base	✓
	Notification of assets found through Attack Surface Management (ASM)	✓
	Addition and tagging of new assets found through ASM into scans and schedules	✓
CHANGE MANAGEMENT	Update control to customers environment	✓
	Change approval	✓
RELEASE MANAGEMENT	Patch and update Tenable scanning software deployed	✓
	Auto system updates based on SaaS Tenable platform	✓
	Proactive Maintenance: Regular health checks and maintenance of the Tenable deployment to ensure optimal performance.	✓
SERVICE REQUEST	Ad hoc vulnerability schedules and scans	✓
	Amending new schedules and scans	✓

Service	Deliverables	Fully Managed
	Asset Discovery: Comprehensive discovery and inventory of all assets, including on-premises, cloud, and hybrid environments.	✓
	Agent-Based Scanning: Supporting the customers deployment of Tenable agents for continuous and in-depth scanning of endpoints.	✓
	Executive Dashboards: Customer request high-level dashboards for executives to get an overview of the security posture.	✓
	Detailed Technical Reports: Customer request comprehensive reports for IT and security teams, including vulnerability details, affected assets, and remediation steps.	✓
SERVICE HOURS	Service Management during UK Working hours, Monday to Friday 09:00 to 17:00, excluding UK Bank holidays and weekends	✓
	Out of hours Emergency Scans placed with MTI 24 x 7 x 365 (up to 4 x Emergency Scan requests included per quarter)	✓
Engineering & Consultancy (Chargeable)	a) Engineering & Consultancy Days – Bought upfront and consumed against service deliverables b) Dashboard customisations * c) Additional Onboarding * d) Dashboard Training * e) Remediation Management – comprising coordinated follow-up with resolver teams to ensure vulnerabilities are prioritised and fixed within agreed SLAs, providing oversight, tracking progress, and driving accountability to ensure issues are resolved on-time.	* Inclusive within the Service **Optional** Remediation Management is chargeable

9.0 APPENDIX – TENABLE ONE LICENSING

TENABLE ONE ASSET VALUES

Tenable One has a centralized platform approach, collecting data from many asset types and providing domain-specific security teams (for example, Tenable Vulnerability Management, Tenable Cloud Security) with specialized domain-specific applications. These applications are like point products for managing cloud, web applications, OT assets, and so on, enhanced with context from the Tenable One platform.

The value customers derive from Tenable One varies by the type of resource being managed, as does the cost incurred by Tenable. To align Tenable One pricing to value, we convert the number of different resource types (for example, web servers, cloud resources, OT devices) to a number of Tenable One assets based on ratios defined in the following table. In this way we maintain a single price per Tenable One asset no matter the variety of resources being managed.

The following table defines the Tenable One asset types in each product and compares them to their Tenable One *asset value*, which is the number of licenses you purchase from Tenable.

Note: Tenable Lumin, Lumin Exposure View, Tenable Inventory, and Attack Path Analysis are included in Tenable One and do not require separate licenses.

The current licensing model in force and applicable to quotations and contracts is detailed at the URL below: https://docs.tenable.com/quick-reference/licensing-guide/Content/tenable-one-licensing.htm

An extract is included below:

Product	Definition	Tenable One Asset Value
Tenable Vulnerability Management	Assets are scanned targets from the past 90 days, discovery excluded or imported assets with vulnerabilities. Examples include hosts, IP addresses, or other targets.	1 of your assets equals 1 Tenable One asset.
Tenable Security Center+		1 IP address in your environment equals 1 Tenable One asset.
Tenable Web App Scanning	Assets are fully qualified domain names (FQDNs) assessed in the past 90 days. If you only scan IP addresses, those are used instead.	1 FQDN or IP address in your environment equals 1 Tenable One asset.
Tenable Identity Exposure	Assets are human or machine identities in your identity service, for example: users, devices, applications, or systems.	1 identity asset in your environment equals 0.50 Tenable One assets.
Tenable Cloud Security CIEM	In Tenable Cloud Security, the assets you license are called *billable assets*. Billable assets are based on public cloud compute instances, public cloud container hosts or orchestrators, serverless assets, container repositories or on-premises container hosts.	1 Tenable Cloud Security CIEM billable asset equals 3 Tenable One assets.
Tenable Cloud Security Standard		1 Tenable Cloud Security Standard billable asset equals 5 Tenable One assets.

Tenable Cloud Security Enterprise		1 Tenable Cloud Security Enterprise billable asset equals 7.50 Tenable One assets.
Tenable OT Security	Assets are detected devices with IP addresses, a single license for each IP address.	1 detected device in your environment equals 1.50 Tenable One assets.
Tenable Attack Surface Management Fortnightly Frequency	Assets are observable objects, which are domain names, subdomains, or IP addresses for internet-connected or internal network devices.	1 observable object in your environment equals 0.25 Tenable One assets.
Tenable Attack Surface Management Daily Frequency		1 observable object in your environment equals 0.50 Tenable One assets.

Tenable One Calculator

Use this calculator to estimate your license needs. In the **Licenses** column, enter your assets. The number of Tenable licenses to purchase appears in the **Assets** column. You must buy at least 300 licenses at a time.

Tip: *Licenses* is the number of assets in your environment that you want to manage in Tenable One. *Assets* is the number of Tenable One assets that you need to purchase.

Warning: This calculator provides an *estimate* and cannot be used for a sales quote. To get a sales quote, contact your Tenable representative.

Product	Type	Licenses	Ratio	Assets
Cloud Products				
Tenable Vulnerability Management	Assets		1.00	0.00
Tenable Web App Scanning	FQDNs		1.00	0.00
CIEM	Cloud resource workloads		3.00	0.00
Tenable Cloud Security Standard	Cloud resource workloads		5.00	0.00
Tenable Cloud Security Enterprise	Cloud resource workloads		7.50	0.00
Tenable Identity Exposure	Identities		0.50	0.00
Tenable Attack Surface Management Fortnightly Frequency	Observable objects		0.25	0.00

Tenable Attack Surface Management Daily Frequency	Observable objects		0.50	0.00
On-premises Products				
Tenable OT Security	Assets		1.50	0.00
Tenable Web App Scanning	FQDNs		1.00	0.00
Tenable Security Center+	IP addresses		1.00	0.00
Third-Party Applications				
Third-Party Application Assets	Assets		0.5	0.00
Totals				
Total Tenable One Cloud Assets		300.00		
Total Tenable One On-premises Assets		0.00		
Total Third-Party Application Assets		0.00		
Total Tenable One Assets		300.00		

Reclaiming Licenses

When you purchase Tenable licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable One products reclaim licenses under some conditions—and then reassign them to new assets in the same product so that you do not run out of licenses.

The following table explains how each Tenable One product reclaims licenses.

Product	License Reclamation Process
Tenable Vulnerability Management	Licenses from deleted assets are reclaimed within 24 hours. Licenses for assets on a network with Asset Age Out enabled are reclaimed after not being scanned for a length of time you specify. Licenses for all other assets are reclaimed after not being scanned for 90 days.
Tenable Web App Scanning	Licenses from deleted assets are reclaimed within 24 hours. Licenses for assets that age out are reclaimed after a length of time you specify, or after 90 days.
Tenable Security Center	Licenses are reclaimed when you delete a repository, run a license report, or upload a new license. If you set assets to age out, licenses are reclaimed during nightly cleanup. If you configure your scan settings to remove unresponsive hosts, licenses are reclaimed at scan import. For more information, see License Count in the *Tenable Security Center Best Practices Guide*.

Tenable Identity Exposure	Licenses for enabled users you delete are reclaimed in real time when removed from your environment's directory service.
Tenable OT Security	Licenses for hidden assets are reclaimed in real time, as are licenses for assets that have been offline for more than 30 days. Licenses for assets you remove or hide in the user interface are also reclaimed.
Tenable Attack Surface Management	Licenses are reclaimed when individual assets are acquired when asset sources are removed or age out. Your license count is updated daily.

Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, Tenable One licenses are elastic. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable One.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable One.
You scan more assets than are licensed for 45+ days.	A message appears in Tenable One; scan and export features are disabled.

Tip: Improper scan hygiene or product misconfigurations can cause scan overages, which result in inflated asset counts. To learn more, see Scan Best Practices.

Expired Licenses

The Tenable One licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform

10.0 ABOUT MTI

MTI Technology is a technology services and solutions provider with over 200 staff, operating across EMEA with offices in the UK and Germany. Over the last 36 years, MTI has helped thousands of organisations transform their IT operations, enabling them to leverage the latest technologies, reduce operating costs, become more flexible, and mitigate risk.

MTI has considerable experience in designing, delivering, and managing cybersecurity and data centre solutions for our customers across various industry sectors, including Commercial, NHS, central government, local government, Banking, Defence, Finance, and Insurance. This extensive experience ensures your solution is designed and installed by industry-leading MTI experts, guaranteeing a smooth, accurate, and on-time project delivery.

MTI specialise in cybersecurity, data centre modernisation, IT managed services and IT transformation. By employing proven methodologies and best practices, and adopting a consultative approach, MTI helps its customers solve business challenges and provides secure, compliant management of their applications, data, infrastructure, and system environments.

ACCREDITATIONS

MTI hold the following ISO Standards and Certifications

- ISO 27001 Information Security Management system
- ISO 9001 Quality Management System
- ISO 20000 IT Service Management
- ISO 45001 Occupational Health and Safety Management
- ISO 22301 Business Continuity Management System
- ISO 14001 Environmental Management System
- Cyber Essentials & Cyber Essentials Plus
- NCSC CHECK Scheme Member (CHECK 'Green Light' company since 2003)
- CREST Scheme Member

AWARDS

Our dedication to maintaining high standards is reflected in our numerous industry awards, including Dell Specialist Partner of the Year 2024, Dell Exceptional Services Delivery Performance 2024, Dell Advanced Services Delivery Partner 2024, Cyber Security Customer Service Award at the Computing Security Awards 2024, Cybersecurity/Data Protection Partner of the Year Award at the CRN Awards 2024, CRN MSSP/Security Reseller of the Year 2023, CRN Security Value Added Reseller (VAR) of the year for 2018, 2019, and 2020, and Penetration Tester of the Year for 2018 and 2020. We have won the UK Service Partner of the Year award twice for excellence in service delivery, in 2023/2024. MTI is committed to delivering exceptional customer service, which is why we have an industry-leading 98% customer satisfaction rating.

KEY PLATFORMS

MTI is proud to be a Dell Technologies Titanium Black Partner, the highest tier in Dell's Global Partner Program. This elite recognition positions MTI among a select group of global partners that demonstrate exceptional technical expertise, strategic alignment, and a consistent ability to deliver transformational outcomes for customers in today's data-driven, multi-cloud world.

Other key partners include:

Microsoft Sentinel

Microsoft Defender XDR

Quest

VEEAM

BROADCOM PREMIER PARTNER VMware Reseller VMWARE DIVISION

TREND Expert

rubrik Authorised Partner

paloalto NETWORKS Innovator Partner

PURESTORAGE

CYBERARK

LevelBlue Authorised Partner

aws

Microsoft Azure

CISCO

tenable

f5

PC Partner Lenovo Platinum PFH

Authorised Reseller PFH

logitech PFH

SAMSUNG PFH

Hewlett Packard Enterprise PFH

KnowBe4 Human error. Conquered.

Forcepoint

FORTINET

SOPHOS

CYBERARK

CROWDSTRIKE

COMMVAULT MARKETBUILDER

SOPHOS

COMMVAULT

Check Point SOFTWARE TECHNOLOGIES LTD

ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG), CSR & SOCIAL VALUE

MTI integrates ESG, CSR and Social Value principles into our business values and operations to meet the expectations of customers, employees, investors, suppliers, the community, and the environment. Our Policy governs responsible and ethical conduct, a positive working environment, support for local communities, fair dealings with suppliers, and respect for human rights.

Environmental Management

MTI maintains a documented Environmental Policy Statement, approved by senior leadership, and reviewed annually. Our **ISO 14001 Environmental Management System** incorporates policies and procedures to manage, reduce, and report environmental impacts. We are committed to **Net Zero by 2050** and have achieved **EcoVadis Gold** standard for Social Value policies and procedures.

Sustainability Activities and Achievements

- **Planting of ~600 trees annually** to neutralise our carbon footprint (in partnership with Treedom). Treedom plants a tree on our behalf across Africa, South-East Asia, and South America to offset MTI's carbon emissions. They are a certified B Corporation, and every tree on their site has its own online page for tracking. To date, MTI has planted 3,299 trees, resulting in a 6.17 mt CO2e reduction and driving positive social and environmental impact.
- Reduction targets for business travel, including a digital-first approach, increased virtual meetings, and reduced travel emissions.
- **In 2023, we took one step closer as we are proud to say all our company vehicles are electric.**
- Transition to homeworking/hybrid models, reducing commuting and office energy consumption.
- Use of renewable energy sources for office electricity and optimisation of lighting, heating, and cooling systems.
- Eradication of single-use plastics in all offices.
- Implementation of cloud-based applications to reduce energy consumption.
- Collaboration with carbon-neutral suppliers and annual Supplier Sustainability Assessments.
- Comprehensive waste management systems, with recycling and mandatory staff training.
- Ongoing achievement of ISO 14001:2015 Certification.

Social Responsibility and Value Creation

- Dedicated ESG committee overseeing strategy, risk management, compliance, stakeholder engagement, and continuous improvement.
- Social Value Development Plan tracked by an ESG Manager, with regular reviews and reporting.
- Employer-supported volunteering, offering employees charity days tracked via our ESG application. MTI employees have completed 1,088 hours of volunteering.
- Initiatives supporting disadvantaged groups, including participation in the Disability Confident Scheme.

- Commitment to equal opportunity, diversity, and inclusion in the workplace.
- MTI support Cystic Fibrosis Charity through fundraising events, employee challenges, and donations.

Governance and Assurance

- Regular supplier assurance activities and annual Supplier Code of Conduct refresh.
- Compliance with ILO standards, UN Global Compact, and Universal Declaration of Human Rights.
- Board-level reporting of CSR compliance and performance.

Public Disclosure and Transparency

- Annual publication of Carbon Reduction Plan/ESG Report on MTI's website - https://mti.com/about/corporate-social-responsibility/
    - https://mti.com/wp-content/uploads/2025/10/MTI_Carbon-Reduction-Plan_FY2024.pdf
- Enhanced reporting of ESG performance and promotion of industry certifications - https://mti.com/wp-content/uploads/2025/12/ESG-Report-FY24.pdf

Head Office

MTI Technology Limited

3 Lotus Park First Floor

The Causeway

Staines-Upon-Thames

TW18 3AG

Reception: +44 (0) 1483 520 200

Service Desk: +44 (0) 1483 520 349

Web: www.mti.com

About MTI

MTI provides award-winning, end-to-end technology solutions and services across cybersecurity and data centre infrastructure, supporting customers for over 35 years. With over 250 specialists across the UK, France, and Germany, we deliver expert consultancy, project delivery, and scalable managed services.

Our mission is to build a secure digital future for our customers. We do this by combining deep technical expertise with a consultative, proven approach – helping organisations accelerate and de-risk transformation while ensuring secure, compliant management of applications, data, and IT systems.